UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/474,203	12/29/1999	YUNZHOU LI	2204/198	1987

7590 01/25/2006

STEUBING MCGUINNESS & MANARAS LLP
125 Nagog Park Drive
Acton, MA 01720

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 01/25/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/474,203	LI ET AL.	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 January 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-49* is/are pending in the application.

4a) Of the above claim(s) *5,19,30,38 and 46* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4, 6-18, 20-29, 31-37, 39-45, and 47-49* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-49 have been re-examined and are pending.

Claims 5, 19, 30, 38, and 46 have been cancelled.

This is a Final rejection.

2. Response to argument.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. ***Claims 1-4, 6-8, 15-18, 20-22, and 26-29, 31-37, 39-45, and 47-49 are rejected under 35 U.S.C. 102(b) as being anticipated by Mittra (US 5,748,736).***

As per claim 1:

Mittra teaches a method of implementing multicast security **(col.6, lines 56-61)** in a given multicast domain, the given multicast domain having one or more network devices, the method comprising: **[see FIGs.1-3, shows multiple multicast networks (domains) having the servers (network devices)]**

receiving multicast traffic that is encrypted with a global key **[col.9, lines 48-67; Mittra discusses that the multicast messages must be encrypted when being sent to the given multicast group (domains) from the senders]**, the global key being available to the given multicast domain and one or more other multicast domains; **[col.6, lines 2-66; the secure multicast group is controlled by a single group security controller (GSC) of FIG.1-3 which shows the multicast group is not being referred as one domain but implies that the group consists of multiple multicast networks (domains). Thus concludes that the group key is for the given one domain and other multiple domains]**

decrypting the receive multicast traffic with the global key to produce decrypted multicast traffic; **[col.10, lines 48-50[**

encrypting the decrypted multicast traffic with a local key to produce local encrypted multicast traffic, the local key being available only to the given multicast domain; and **[col.10, lines 20-21 and lines 48-51]**

forwarding the local encrypted multicast traffic to the one or more network devices in the given multicast domain. **(col.12, lines 55-59)**

As per claim 2: See **col.9, lines 63-65;** discusses receiving a global key message that identifies the global key.

As per claim 3: See **col.12, lines 39-59;** discusses local encrypted multicast traffic is forwarded to all of the network devices in the given multicast domain.

As per claim 4: See **col.5, lines 1-3 and col.13, lines 4-7;** discusses the local encrypted multicast traffic is forwarded to a subset of the network devices in the given multicast domain, the subset of network devices being identified in a multicast message.

As per claim 5: Cancelled

As per claim 6: See **col.7, lines 1-13;** discusses the given multicast domain is a protocol independent multicast domain.

As per claim 7: See **col.6, line 39 thru col.7, line 13;** discusses the given multicast domain is a group of contiguous protocol independent multicast domains.

As per claim 8: See **col.6, lines 4-15;** discusses the given multicast domain is part of a Multicast Source Discovery Protocol backbone.

As per claim 15:

A method of implementing multicast security in a network, the method comprising:

encrypting multicast traffic with a global key **[col.9, lines 48-67; Mittra discusses that the multicast messages must be encrypted when being sent to the given multicast group (domains) from the senders]**, the global key being available to the given multicast domain and one or more multicast domains; **[col.6, lines 2-66; the secure multicast group is controlled by a single group security controller (GSC) of FIG.1-3 which shows the multicast group is not being referred as one domain but implies that the group consists of multiple multicast networks (domains). Thus concludes that the group key is for the given one domain and other multiple domains]**

forwarding the global encrypted multicast traffic to the given multicast domain; **[col.9, lines 64-65]**

receiving the global encrypted multicast traffic at the given multicast domain; **[col.10, lines 18-20]**

decrypting, at the given multicast domain, the global encrypted multicast traffic with the global key to produce decrypted multicast traffic; **[col.10, lines 48-50]**

encrypting, at the given multicast domain, the decrypted multicast traffic with a local key to produce local encrypted multicast traffic, the local key being available only to the given multicast domain; and **[col.10, lines 20-21 and lines 48-51; the key that the sender shares with the GSC is the local key which is unique to that (one) sender and the GSC, thus is unlike the group key where multiple senders or groups of domains shares the key with the GSC.]**

forwarding the local encrypted multicast traffic to the one or more network devices in the given multicast domain. **[col.12, lines 55-59]**

As per claim 16: See **col.9, lines 63-65;** discusses receiving at the given multicast domain a global key message that identifies the global key.

As per claim 17: See **col.12, lines 39-59;** discusses the local encrypted multicast traffic is forwarded to all of the network devices in the given multicast domain.

As per claim 18: See **col.5, lines 1-3 and col.13, lines 4-7;** discusses the local encrypted multicast traffic is forwarded to a subset of the network devices in the given multicast domain, the subset of network devices being identified in a multicast message.

As per claim 19: Cancelled

As per claim 20: See **col.7, lines 1-13;** discusses the given multicast domain is a protocol independent multicast domain.

As per claim 21: See **col.6, line 39 thru col.7, line 13;** discusses the given multicast domain is a group of contiguous protocol independent multicast domains.

As per claim 22: See **col.6, lines 4-15;** discusses the given multicast domain is part of a Multicast Source Discovery Protocol backbone.

As per claim 26:

Mittra an apparatus for implementing multicast security in a given multicast domain, the given multicast domain having one or more network devices, the apparatus comprising:

a receiver for receiving multicast traffic that is encrypted with a global key **[col.9, lines 48-67; Mittra discusses that the multicast messages must be encrypted when being sent to the given multicast group (domains) from the senders]**, the global key being available to the given multicast traffic with the global key to produce decrypted multicast traffic; **[col.6, lines 2-66; the secure multicast group is controlled by a single group security controller (GSC) of FIG.1-3 which shows the multicast group is not being referred as one domain but implies that the group consists of multiple multicast networks (domains). Thus concludes that the group key is for the given one domain and other multiple domains]**

a decryptor for decrypting the receive multicast traffic with the global key to produce decrypted multicast traffic **[col.10, lines 48-50]**

an encryptor for encrypting the decrypted multicast traffic with a local key to produce local encrypted multicast traffic, the local key being available only **(col.10, lines 45-52 and col.12, lines 55-59)** to the given multicast domain; and **[col.10, lines 20-21 and lines 48-51]**

a traffic forwarder for forwarding the local encrypted multicast traffic to the one or more network devices in the given multicast domain. **[col.12, lines 40-53]**

As per claim 27: See **col.9, lines 63-65;** discusses a second receiver for receiving a global key message that identifies the global key.

As per claim 28: See **col.12, lines 39-59;** discusses the local encrypted multicast traffic is forwarded to all of the network devices in the given multicast domain.

As per claim 29: See **col.5, lines 1-3 and col.13, lines 4-7;** discusses the local encrypted multicast traffic is forwarded to a subset of the network devices in the given multicast domain, the subset of network devices being identified in a multicast message.

As per claim 30: Cancelled

As per claim 31: See **col.7, lines 1-13;** discusses the apparatus according to claim 26 wherein the given multicast domain is a protocol independent multicast domain.

As per claim 32: See **col.6, line 39 thru col.7, line 13;** discusses the given multicast domain is a group of contiguous protocol independent multicast domains.

As per claim 33: See **col.6, lines 4-15;** discusses the given multicast domain is part of a Multicast Source Discovery Protocol backbone.

As per claim 34:

Mittra teaches a computer program product for implementing multicast security in a given multicast domain, the given multicast domain having one or more network devices, the computer comprising:

program code for receiving multicast traffic that is encrypted with a global key **[col.9, lines 48-67; Mittra discusses that the multicast messages must be encrypted when being sent to the given multicast group (domains) from the senders]**, the global key being available to the given multicast traffic with the global key to produce decrypted multicast traffic; **[col.6, lines 2-66; the secure multicast group is controlled by a single group security controller (GSC) of FIG.1-3 which shows the multicast group is not being referred as one domain but implies that the group consists of multiple multicast networks (domains). Thus concludes that the group key is for the given one domain and other multiple domains]**

program code for decrypting the receive multicast traffic with the global key to produce decrypted multicast traffic **[col.10, lines 48-50]**

program code for encrypting the decrypted multicast traffic with a local key to produce local encrypted multicast traffic, the local key being available only **(col.10, lines 45-52 and col.12, lines 55-59)** to the given multicast domain; and **[col.10, lines 20-21 and lines 48-51; the key that the sender shares with the GSC is the local key which is unique to that (one) sender and the GSC, thus is unlike the group key where multiple senders or groups of domains shares the key with the GSC.]**

program code for forwarding the local encrypted multicast traffic to the one or more network devices in the given multicast domain. **[col.12, lines 40-53]**

As per claim 35: See **col.9, lines 63-65;** discusses a program code for receiving a global key message that identifies the global key.

As per claim 36: See **col.12, lines 39-59;** discloses the local encrypted multicast traffic is forwarded to all of the network devices in the given multicast domain.

As per claim 37: See **col.5, lines 1-3 and col.13, lines 4-7;** discusses the local encrypted multicast traffic is forwarded to a subset of the network devices in the given multicast domain, the subset of network devices being identified in a multicast message.

As per claim 38: See **col.10, lines 45-52 and col.12, lines 55-59;** discusses the local key is only available to the given multicast domain.

As per claim 39: See **col.7, lines 1-13;** discusses the given multicast domain is a protocol independent multicast domain.

As per claim 40: See **col.6, line 39 thru col.7, line 13;** discusses the given multicast domain is a group of contiguous protocol independent multicast domains.

As per claim 41: See **col.6, lines 4-15;** discusses the given multicast domain is part of a Multicast Source Discovery Protocol backbone.

As per claim 42:

Mittra teaches an apparatus of implementing multicast security in a network, the apparatus comprising:

means for encrypting multicast traffic with a global key **[col.9, lines 48-67; Mittra discusses that the multicast messages must be encrypted when being sent to the**

given multicast group (domains) from the senders], the global key being available to only **(col.10, lines 45-52 and col.12, lines 55-59)** the given multicast domain and one or more multicast domains; **[col.6, lines 2-66; the secure multicast group is controlled by a single group security controller (GSC) of FIG.1-3 which shows the multicast group is not being referred as one domain but implies that the group consists of multiple multicast networks (domains). Thus concludes that the group key is for the given one domain and other multiple domains]**

means for forwarding the global encrypted multicast traffic to the given multicast domain; **[col.10, lines 15-19]**

means for receiving the global encrypted multicast traffic at the given multicast domain; **[col.13, lines 4-7]**

means for decrypting, at the given multicast domain, the global encrypted multicast traffic with the global key to produce decrypted multicast traffic; **[col.10, lines 48-50]**

means for encrypting, at the given multicast domain, the decrypted multicast traffic with a local key to produce local encrypted multicast traffic, the local key being available to the given multicast domain; and **[col.10, lines 20-21 and lines 48-51; the key that the sender shares with the GSC is the local key which is unique to that (one) sender and the GSC, thus is unlike the group key where multiple senders or groups of domains shares the key with the GSC.]**

means for forwarding the local encrypted multicast traffic to the one or more network devices in the given multicast domain. **[col.12, lines 40-53]**

As per claim 43: See **col.9, lines 63-65;** discusses receiving at the given multicast domain a global key message that identifies the global key.

As per claim 44: See **col.12, lines 39-59;** discusses the local encrypted multicast traffic is forwarded to all of the network devices in the given multicast domain.

As per claim 45: See **col.5, lines 1-3 and col.13, lines 4-7;** discusses the local encrypted multicast traffic is forwarded to a subset of the network devices in the given multicast domain, the subset of network devices being identified in a multicast message.

As per claim 46: Cancelled

As per claim 47: See **col.7, lines 1-13;** discusses the given multicast domain is a protocol independent multicast domain.

As per claim 48: See **col.6, line 39 thru col.7, line 13;** discusses the given multicast domain is a group of contiguous protocol independent multicast domains.

As per claim 49: See **col.6, lines 4-15;** discusses the given multicast domain is part of a Multicast Source Discovery Protocol backbone.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. *Claims 9-14 and 23-25 are rejected under 35 U.S.C. 103(a) as being unpatentable by Haggerty, Et Al. (US 6,331,983) in further view of "The Microsoft Computer Dictionary, 5th Edition".*

As per claim 9:

Haggerty, Et. Al. teaches a method of implementing multicast security in a given multicast domain, the method comprising sending packets (containing a destination address) to the group address corresponding to the multicast group indicates the multicast group consists of more than one domain. Haggerty determines whether that the given multicast domain contain no network devices interested in the received multicast traffic **[col.31, lines 35-40]**; and in the event that the given multicast sends a terminate message to no longer forward the received multicast traffic to the give multicast domain **[col.31, line 42 thru col.32, line 15].** However, Haggerty did not fully include encryption for the multicast traffic with the global key.

"The Microsoft Computer Dictionary, 5th Edition" discloses encryption prevents unauthorized access because it is in an unreadable form which usually based on one or more keys to decode to become readable form **[pg.192].**

Therefore, it would have been obvious of one of the ordinary skill in the art to combine the teachings of Haggerty with "The Microsoft Computer Dictionary, 5th Edition", to receive the multicast traffic encrypted with a global key because the multicast traffic with the global key is in unreadable form to prevent unauthorized access.

As per claim 10: **See col.23, lines 30-40;** Haggerty discusses receiving a global key message that identifies the global key.

As per claim 11:

Haggerty discusses determining, after having sent the terminate message, that the given multicast domain contains one or more network devices interested in the received multicast traffic **[col.29, lines 50-52) and** sending a resume message to once again forward the received multicast traffic to the given multicast domain. **[col.29, lines 52-54]**

As per claim 12: See **col.14, lines 28-52;** discusses the given multicast domain is a protocol independent multicast domain.

As per claim 13: See **col.14, lines 28-52;** discusses the given multicast domain is a group of contiguous protocol independent multicast domains.

As per claim 14: See **col.11, lines 38-63;** discusses the given multicast domain is part of a Multicast Source Discovery Protocol backbone.

As per claim 23:

Haggerty teaches constructing in response to the received multicast traffic, an information message that alerts other multicast domains of the security capabilities of the give multicast domain **[col.29, lines 25-26]** and forwarding the information message to at least one other multicast domain **[col.29, lines 27-32]**. However, Haggerty did not fully include encryption for the multicast traffic with the global key.

"The Microsoft Computer Dictionary, 5th Edition" discloses encryption prevents unauthorized access because it is in an unreadable form, which usually based on one or more keys to decode to become readable form **[pg.192].**

Therefore, it would have been obvious of one of the ordinary skill in the art to combine the teachings of Haggerty with "The Microsoft Computer Dictionary, 5th Edition", to receive the multicast traffic encrypted with a global key because the multicast traffic with the global key is in unreadable form that would prevent unauthorized access.

As per claim 24: See **col.14, lines 28-52;** discusses the information message is a part of a multicast protocol message.

As per claim 25: See **col.29, lines 20-32;** discusses one or more bits in one or more fields of the multicast protocol message are set to alert other multicast domains of the security capabilities of the give multicast domain.

Response to Arguments

5. Applicant's arguments filed January 27, 2005 have been fully considered but they are not persuasive.

Mittra discloses a system for secure group communications via multicast transmission (col.59-62) wherein the senders must encrypt the multicast messages when being sent to the given multicast group (col.9, lines 48-67) and further discusses the secure multicast group is controlled by a single group security controller (GSC of FIG.1-3), which shows the multicast group is not being referred to as one of the multicast networks (domains) but implies that the group consists of multiple multicast networks which involves more than one systems, senders, or domains. Thus concludes that the group key is for the given one domain and other multiple domains (col.6, lines 2-66). Mittra discusses the key that the sender shares with the GSC is the local key which is unique to that (particular) sender and the GSC, thus is unlike the group key where multiple senders or groups of domains shares the key with the GSC (col.10, lines 20-21 and lines 48-51).

Conclusion

6. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Lha

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100